



## **Governor's Community Outreach – Federal Programs Office (GCO-FPO)**

*Guide for Safeguarding Sensitive Personally Identifiable Information (PII) and the  
Reporting Requirements to Report an Actual or Imminent Breach of PII.*

**July 2020**

## TABLE OF CONTENTS

Introduction.....	3
PII and PPII.....	4
Collecting Sensitive Information.....	5
<i>Grant Administration</i> .....	5
<i>Subgrantees</i> .....	5
Subgrantee Breach Response Plan / Procedures & Reporting Requirements .....	6
<i>Breach Response Team</i> .....	6
<i>Discovery of Breach or Potential Breach</i> .....	6
<i>Identify Applicable Privacy Compliance Documentation</i> .....	6
<i>Information Sharing to Respond to a Breach</i> .....	7
<i>Reporting Requirements</i> .....	7
<i>Assessment of Risk of Harm to Individuals Potentially Affected by a Breach</i> .....	7
<i>Mitigating Risk of Harm to Individuals Potentially Affected by a Breach</i> .....	7
<i>Notifying Individuals Potentially Affected by a Breach</i> .....	8
<i>Tracking and Documenting Breach Response</i> .....	8
<i>Failure to Report Breach or Potential Breach</i> .....	8
Definitions .....	9
Appendix A .....	11
<i>Certification of Compliance with VAWA Statutory Requirements</i> .....	11
Appendix B .....	15
<i>Reporting Template</i> .....	15

## Introduction

The Violence Against Women Act (VAWA), as amended (42 U.S.C. 13925(b)(2)) requires its grantees and its subgrantees to ensure the safety of adult, youth, and child victims of domestic violence, dating violence, sexual assault, or stalking and their families by protecting the confidentiality and privacy of persons receiving services.



The Governor's Community Outreach – Federal Programs Office and its subgrantees are obligated to protect Personally Identifiable Information (PII) to prevent identity theft or other adverse consequences, such as a privacy incident, compromise, or misuse of data. GCO-FPO staff and subgrantees should exercise care when handling all PII. Protected PII (PPII), however, requires special handling due to the increased risk of harm to an individual if it is compromised. The loss or compromise of PPII can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and in rare cases, a risk to personal safety.

On annual basis, GCO-FPO subgrantees must sign the Acknowledgement of Notice of Statutory Requirement to Comply with the Confidentiality and Privacy Provisions of the VAWA, as amended, and submit to GCO-FPO. [See Appendix A](#)

The VAWA requires GCO-FPO and its subgrantees to report an actual or imminent breach of personally identifiable information (PII). The Office on Violence Against Women (OVW) grant require GCO-FPO to report to OVW no later than 24 hours after an occurrence of actual breach, or the detection of an imminent breach. Subgrantees must report the occurrence of an actual breach, or the detection of an imminent breach to GCO-FPO directly no later than 12 hours after the discovery of the breach or detection of imminent breach. Subgrantee breach reporting procedures must include a requirement to report an actual or imminent breach of PII to the GCO-FPO within 12 hours, GCO-FPO will then will then in turn inform the OVW Program Manager.

GCO-FPO and its subgrantees must have written procedures in place to respond in the event of an actual or imminent breach (as defined in OMB M-17-12) if they:

- 1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII) (as defined in 2 C.F.R. 200.79) within the scope of an OVW grant-funded program or activity, or
- 2) use or operate a Federal information system (as defined in OMB Circular A-130).

This guide will help GCO-FPO and its subgrantees to identify PII and PPII, and serve as the GCO-FPO policy on how to respond and report to OVW in the event of an actual or imminent breach.

## PII and PPII

Personally Identifiable Information or PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor.

PII is a form of Protected Information, which includes, but is not limited to, PII and Protected PII.

Protected PII (PPII) is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

PPII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements, including your Social Security number (SSN) and driver's license or state identification number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of an individual (directly or indirectly inferred), are also PPII.

See table.

- When determining the sensitivity of PII, GCO-FPO and subgrantees should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of data fields together.
  - ⇒ For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or zip code.
- PII can become more sensitive when combined with other information.
  - ⇒ For example, name and credit card number are more sensitive and when combined than apart.
  - ⇒ Generally non-PPII, such as a name, might become sensitive in certain contexts, such as on a clinic's patient list.

**Context matters.** This table should not be regarded as an all-inclusive list of sensitive data elements. Context is also import in determining the sensitivity of PII.

For example, a collection of names:

- Is **not** PPII if it is a list, file, query result of:
  - ⇒ attendees at a public meeting or
  - ⇒ stakeholders who subscribe to GCO-FPO distribution list
- Is PPII if it is a list, file, query result of:
  - ⇒ law enforcement personnel, such as investigators, agents, or support personnel, or
  - ⇒ employee performance ratings, or
  - ⇒ employees with overdue mandatory training course completions.



What is PII?
PII includes your name and your work email, address, and phone.
What is Protected PII?
STAND ALONE (Identifying Numbers)
• Social Security numbers
• Driver's license, state ID numbers
• Passport numbers
• Alien Registration numbers
• Financial account numbers
• Biometric identifiers
IN COMBINATION
• Citizenship or immigration status
• Medical information
• Ethnic or religious affiliation
• Personal email, address
• Account passwords
• Last 4 digits of the SSN
• Date of birth
• Criminal history
• Mother's maiden name

## Collecting Sensitive Information

### *Grant Administration*

GCO-FPO must ensure, through its subgrantee monitoring practices, that subgrantees do not include PII in supporting documents for required reporting and/or for expenses and activities related to the charges claimed in a reimbursement or in the monthly contract payment request. To the greatest extent possible, the subgrantee should protect and redact PII in supporting documents before submitting to GCO-FPO. Subgrantees must exercise caution when providing any personal information necessary for GCO-FPO subgrantee monitoring purposes.

### *Subgrantees*

By statute, a grantee or subgrantee may share personally identifying information in three specific circumstances:

1. When the victim provides written, informed, and reasonably time-limited consent to the release of information ("a release");
2. When a statute compels that the information be released; or
3. When a court compels that the information be released.

Releases must be written, informed, reasonably time limited, and signed by the victim or, if appropriate, a parent or guardian. Grantees and subgrantees may not use a blanket release and must specify the scope and limited circumstances of any disclosure. At a minimum, grantees and subgrantees must:

- Discuss with the victim why the information might be shared, who would have access to the information, and what information could be shared under the release;
- Reach agreement with the victim about what information would be shared and with whom; and
- Record the agreement about the scope of the release.

The release must specify the duration for which the information may be shared.

If a statute or court compels the release of information, the grantee or subgrantee releasing the information must (1) make reasonable attempts to provide notice of the release to affected victims and (2) take steps necessary to protect the privacy and safety of persons affected by the release.

Subgrantees shall refrain from providing GCO-FPO personally identifying information, except in cases required by the Department of Administration – Accounting Division (DOA) for the purposes of establishing a vendor account with the Government of Guam. GCO-FPO will not be responsible should DOA experience an actual or imminent breach.

Personally identifiable information shall also be protected when conducting activities with volunteers or procuring services with vendors and/or contractors.

Subgrantees must use the Fair Information Practice Principles as a guideline to determine how to collect and share PII while considering individual privacy. These guidelines include transparency, participation of the individual whose information is being collected, specifying the purpose for collecting and using the information, minimizing the data that is being collected, limiting the use of the data, ensuring data quality and integrity, having security safeguards, and demonstrating

accountability when collecting personal information. Best practices exist that allow the sharing of information while ensuring privacy.<sup>1</sup>

## Subgrantee Breach Response Plan / Procedures & Reporting Requirements

The subgrantee's breach procedures must include a requirement to report actual or imminent breach of PII to GCO-FPO no later than 12 hours after an occurrence of an actual breach, or the detection of an imminent breach.

Subgrantees must ensure that contract terms necessary for the entity to respond to a breach are included in contracts when a contractor collects or maintains entity information on behalf of the entity or uses or operates an information system on behalf of the agency.<sup>2</sup> To the extent that a cooperative agreement<sup>3</sup> or other such instrument requires another organization or entity to perform such functions on behalf of the agency, the agency must similarly ensure that such cooperative agreements and instruments include the following components.

### *Breach Response Team*

The subgrantee agency or the community-based organization (CBO) grant administrator must be a member of the subgrantee's Breach Response Team. The Breach Response Team is responsible for:

1. Reporting of the breach or suspected breach to the agency/CBO director and GCO-FPO.
2. Informing clients/persons affected that their PII has been breached, and what steps they should take to protect their information (informing banks, credit card companies, IRS (if SSN is breached), etc.) and any steps being taken by the agency/CBO to protect the person(s) whose information has been breached.

### *Discovery of Breach or Potential Breach*

Any subgrantee employee or volunteer who discovers or suspects that PII or PPII may have been breached in any way is REQUIRED to report that actual or suspected breach of PII or PPII to a member of the agency/CBO's Breach Response Team. The initial notification must happen no later than 12 hours after an occurrence of an actual breach, or the detection of an imminent breach. The 12-hour notification should occur via a phone call, in person, or via email. A member of the Breach Response Team must in turn immediately, or as soon as possible, notify GCO-FPO. GCO-FPO will in turn, as soon as possible and within 24 hours, inform our OVW Program Manager via email of the breach/possible breach.

A written report on agency/entity letterhead detailing the breach or suspected breach should be submitted to GCO-FPO within 24 hours of discovery. This report should include any information about the data, technology or equipment that was breached or suspected of having been breached, lost, stolen, or otherwise missing.

### *Identify Applicable Privacy Compliance Documentation*

The subgrantee agency or organization suspecting a breach should review all applicable agency privacy compliance documentation to help identify the information that was potentially compromised and

---

<sup>1</sup> NNEDV, Why Privacy and Confidentiality Matters for Victims of Domestic and Sexual Violence

<sup>2</sup> 44 U.S.C. § 3553(a)(1)(A)

<sup>3</sup> 31 U.S.C. § 6305.

the population of individuals potentially affected by the breach. Privacy notices should be accurate and up-to-date.

#### *Information Sharing to Respond to a Breach*

If the agency or entity needs additional information to reconcile or eliminate duplicate records in response to a breach, identify potentially affected individuals, or obtain contact information in order to provide notification, the agency must consider whether any information that must be shared is consistent with current data use agreements, or whether the information sharing will require new data use agreements or information exchange agreements. The agency must also ensure that any new PII gathered is protected from additional breaches. Subgrantee must cooperate with regard to the exchange of information with GCO-FPO and with Federal Awarding agency officials, as needed, to properly refer and respond to a breach.

#### *Reporting Requirements*

Upon evaluation of the breach by the agency or entity's Breach Response Team, the agency shall, if necessary, notify law enforcement officials of the breach, and if necessary, notify other oversight entities that will need to be apprised of the breach incident. When a breach warrants a report to law enforcement, the agency/CBO shall ensure that the report is promptly submitted, even if the breach is unconfirmed or if circumstances are unclear. Prompt referral to law enforcement can prevent PII from being further compromised and in some cases reduce the risk of harm to potentially affected individuals.

#### *Assessment of Risk of Harm to Individuals Potentially Affected by a Breach*

The Breach Response Team shall also, as soon as possible after the 12-hour notification to the agency head and GCO-FPO, conduct and document an assessment of the risk of harm to individuals potentially affected by a breach. This assessment must include the factors being considered when assessing the risk, such as the amount and type of information that was breached, and consideration of any potential harm that could result from the breach, such as breach of confidentiality, fiduciary responsibility, potential for blackmail, disclosure of private facts, mental pain and emotional distress, financial harm, disclosure of contact information for victims of abuse, the potential for secondary uses of information which could result in fear or uncertainty, humiliation, or loss of self-esteem for the client.

Additionally, the federal Privacy Act of 1974 requires agencies to protect against any anticipated threats or hazards to the security or integrity of records that could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, as well as risks to the agency, agency information systems, programs and operations."

The following factors should be considered when assessing risks relevant to the breach:

- Nature and sensitivity of the PII potentially compromised by the breach;
- Likelihood of access and use of the PII;
- Type of breach (including circumstances of the breach, actors (if known) and their intent (if known)).

#### *Mitigating Risk of Harm to Individuals Potentially Affected by a Breach*

Once the breach is assessed, the Breach Response Team shall consider and take action to best mitigate the identified risks to clients or individuals whose PII may have been compromised.

The team is responsible for advising the head of the agency or CBO, and the agency's IT team, if applicable, on whether to take countermeasures (such as changing passwords or placing an alert in a database containing potentially compromised PII), offer guidance (on setting up fraud alerts to a bank account, putting a freeze on a credit card, etc.), or provide services (such as credit monitoring) to individuals potentially affected by the breach.

### *Notifying Individuals Potentially Affected by a Breach*

The Breach Response Team and the agency or CBO head must decide, depending on the circumstances of the breach, on when to notify individuals potentially affected by a breach. Ultimately, the decision of when and how to notify individuals of a breach of PII or a potential breach rests with the head of the agency or CBO.

With regard to notification, the need for transparency must be balanced with concerns about over-notification. Notification of the public about a breach may not always be helpful and may in fact bring undo attention to individuals who are recipients of services provided by the STOP or SASP grants.

In circumstances where the information involved in the breach is subject to other requirements (for example the Health Insurance Portability and Accountability Act (HIPAA)), appropriate subject matter experts should be brought in as part of the Breach Response Team.

Any notification should consider the following:

- Source of the notification, including the person from the agency designated to notify the individuals potentially affected by the breach;
- Timeliness of the notification (delays may cause undo harm to the individual emotionally, financially, or otherwise)
- Contents of the notification
- Method of notification (depending on the circumstances of the breach)
- Special considerations (tailoring notifications to specific populations, how to notify those visually or hearing impaired, etc.)

### *Tracking and Documenting Breach Response*

Subgrantees are required to formally track and document each breach that is reported to the agency or CBO, through a standard internal reporting template. A reporting template is attached for your consideration ([Appendix B](#)). This formal documentation serves to ensure that notification and any mitigation steps occur in a timely manner, and should include the status of the breach and its outcome.

### *Failure to Report Breach or Potential Breach*

Any subgrantee employee or volunteer who fails to notify a member of his/her organization/CBO's Breach Response Team after having learned of a breach or suspected breach may be subject to subgrant award suspension or termination, as appropriate.

## Definitions

### **Breach**

OMB M-17-12

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

### **Community-Based Organization**

34 U.S. Code § 12291

A nonprofit, nongovernmental, or tribal organization that serves a specific geographic community that –

- (A) focuses primarily on domestic violence, dating violence, sexual assault, or stalking;
- (B) has established a specialized culturally specific program that addresses domestic violence, dating violence, sexual assault, or stalking;
- (C) has a primary focus on underserved populations (and includes representatives of these populations) and domestic violence, dating violence, sexual assault, or stalking; or
- (D) obtains expertise, or shows demonstrated capacity to work effectively, on domestic violence, dating violence, sexual assault, and stalking through collaboration.

*For the purposes of this document, a community-based organization is interchangeably known as a STOP and/or SASP subgrantee that is a nongovernmental organization and/or a non-profit organization.*

### **Contractor**

2 C.F.R. § 200.23

An entity that receives a contract.

### **Contract**

2 C.F.R. § 200.22

A legal instrument by which a non-Federal entity purchases property or services to carry out the project or program under a Federal award. The term as used in this part does not include a legal instrument, even if the non-Federal Entity considers it a contract, when the substance of the transaction meets the definition of a Federal award or subaward.

### **Incident**

OMB M-17-12

An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

### **Information Security**

Means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) availability, which means ensuring timely and reliable access to and use of information.

### **Pass-through Entity**

2 C.F.R. § 200.74

A non-Federal entity that provides a subaward to a subrecipient (subgrantee) to carry out part of a Federal program.

For the purposes of this document, the pass-through entity is also known as the Governor's Community Outreach – Federal Programs Office, the State Administering Agency for the STOP and SASP Formula Grant Awards.

### **Personally Identifiable Information (PII)**

2 C.F.R. § 200.79

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites,

and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

**Protected Personally Identifiable Information (Protected PII)**

2 C.F.R. § 200.82

Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.

**Subaward**

2 C.F.R. § 200.92

An award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal Award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

**Termination**

2 C.F.R. § 200.95

The ending of a Federal award, in a whole or in part at any time prior to the planned end of period of performance. For the purposes of this section, the term federal award is in reference to subrecipient, subgrantee (governmental or CBO).

## Appendix A

### *Certification of Compliance with VAWA Statutory Requirements*

OMB Number – 1122-0001  
Expiration Date: 04/30/2022

**U.S. Department of Justice**  
*Office on Violence Against Women*



---

### **Certification of Compliance with the Statutory Eligibility Requirements of the Violence Against Women Act as Amended, STOP Formula Grant Program**

---

Applicants should refer to the laws cited below for further information regarding the certifications to which they are required to attest. Signature on this form certifies that the applicant is qualified to receive the STOP Formula Grant Program funds and is in compliance with relevant requirements under 34 U.S.C §§ 10441, 10446 through 10451 and 28 C.F.R. Part 90. These certifications shall be treated as a material representation of fact upon which the Department of Justice will rely if it determines to award the covered transaction, grant, or cooperative agreement.

Upon complying with the application requirements set forth in the solicitation, any state (or territory) shall be qualified for funds provided under the STOP Formula Grant Program upon certification that:

- (1) the funds will be used only for the statutory purposes described in 34 U.S.C. § 10441(a) and (b);
- (2) grantees and subgrantees will develop plans for implementation and will consult and coordinate with:
  - (A) the State sexual assault coalition;
  - (B) the State domestic violence coalition;
  - (C) the law enforcement entities within the State;
  - (D) prosecution offices;
  - (E) State and local courts;
  - (F) Tribal governments in those States with State or federally recognized Indian tribes;
  - (G) representatives from underserved populations, including culturally specific populations;
  - (H) victim service providers;
  - (I) population specific organizations; and
  - (J) other entities that the State or the Attorney General identifies as needed for the planning process;
- (3) grantees will coordinate the State implementation plan with the State plans described in section 307 of the Family Violence Prevention and Services Act (42 U.S.C. 10407) and the programs described in section 1404 of the Victims of Crime Act of 1984 (34 U.S.C. 20103) and section 393A of the Public Health Service Act (42 U.S.C. 280b-1b).
- (4) the amount granted will be allocated, without duplication, as follows: not less than 25 percent for law enforcement, not less than 25 percent for prosecutors, not less than 30 percent for victim

OMB Number – 1122-0001  
Expiration Date:04/30/2022

services (of which at least 10 percent will be distributed to culturally specific community-based organizations), and not less than 5 percent to state and local courts;  
(5) not later than 2 years after March 7, 2013, and every year thereafter, not less than 20 percent of the total amount granted to a State under this subchapter shall be allocated for programs or projects in 2 or more allocations listed in paragraph (4) that meaningfully address sexual assault, including stranger rape, acquaintance rape, alcohol or drug-facilitated rape, and rape within the context of an intimate partner relationship; and

(6) any federal funds received under this subchapter will be used to supplement, not supplant, nonfederal funds that would otherwise be available for activities funded under this chapter.

In addition, to be eligible for funding under the STOP Formula Grant Program, applicants must certify compliance with the requirements in 34 U.S.C. §§ 10449, 10450, and 10451 and implemented at 28 C.F.R. Part 90, as follows:

**(1) Forensic Medical Examination Payment Requirement for Victims of Sexual Assault**

(a) A state, Indian tribal government, or unit of local government shall not be entitled to funds under the STOP Formula Grant Program unless the state, Indian tribal government, unit of local government, or another governmental entity—

(1) incurs the full out-of-pocket cost of forensic medical exams for victims of sexual assault; and

(2) coordinates with health care providers in the region to notify victims of sexual assault of the availability of rape exams at no cost to the victims.

(b) A state, Indian tribal government, or unit of local government shall be deemed to incur the full out-of-pocket cost of forensic medical exams for victims of sexual assault if any government entity:

(1) provides such exams to victims free of charge to the victim; or

(2) arranges for victims to obtain such exams free of charge to the victims.

(c) A state or Indian tribal government may use STOP Formula Grant Program funds to pay for forensic medical exams performed by trained examiners for victims of sexual assault, except that such funds may not be used to pay for forensic medical exams by any state, Indian tribal government, or territorial government that requires victims of sexual assault to seek reimbursement for such exams from their insurance carriers.

(d) (1) To be in compliance with this section, a state, Indian tribal government, or unit of local government shall comply with subsection (b) without regard to whether the victim participates in the criminal justice system or cooperates with law enforcement.

(2) States, territories, and Indian tribal governments shall have 3 years from March 7, 2013 to come into compliance with this section.

**(2) Filing Costs For Criminal Charges and Protection Orders**

A state, Indian tribal government, or unit of local government will not be entitled to funds under the STOP Formula Grant Program unless it certifies that its laws, policies, and practices do not

OMB Number – 1122-0001  
Expiration Date:04/30/2022

require, in connection with the prosecution of any misdemeanor or felony sexual assault, domestic violence, dating violence, or stalking offense, or in connection with the filing, issuance, registration, modification, enforcement, dismissal, withdrawal or service of a protection order, or a petition for a protection order, to protect a victim of sexual assault, domestic violence, dating violence, or stalking, that the victim bear the costs associated with the filing of criminal charges against the offender, or the costs associated with the filing, issuance, registration, modification, enforcement, dismissal, withdrawal or service of a warrant, protection order, petition for a protection order, or witness subpoena, whether issued inside or outside the State, tribal, or local jurisdiction.

### (3) Judicial Notification

A State or unit of local government shall not be entitled to funds under the STOP Formula Grant Program unless the state or unit of local government—

(a) certifies that its judicial administrative policies and practices include notification to domestic violence offenders of the requirements delineated in section 922(g)(8) and (g)(9) of title 18, United States Code, and any applicable related federal, state, or local laws; or

(b) gives the Attorney General assurances that its judicial administrative policies and practices will be in compliance with the requirements of subparagraph (A) within the later of—

(1) the period ending on the date on which the next session of the state legislature ends; or

(2) January 5, 2008.

### (4) Polygraph Testing Prohibition

(a) In order to be eligible for grants under the STOP Formula Grant Program, a state, Indian tribal government, territorial government, or unit of local government shall certify that, not later than January 5, 2009, their laws, policies, or practices will ensure that no law enforcement officer, prosecuting officer or other government official shall ask or require an adult, youth, or child victim of an alleged sex offense as defined under federal, tribal, state, territorial, or local law to submit to a polygraph examination or other truth telling device as a condition for proceeding with the investigation of such an offense.

(b) The refusal of a victim to submit to a polygraph or other truth telling examination shall not prevent the investigation, charging, or prosecution of an alleged sex offense by a state, Indian tribal government, territorial government, or unit of local government.

---

As the duly authorized representative of the applicant, I hereby certify that the applicant will comply with above certifications.

---

Typed Name of Authorized Representative	Title	Telephone Number
---	-------	------------------

OMB Number – 1122-0001  
Expiration Date:04/30/2022

\_\_\_\_\_  
Signature of Authorized Representative

\_\_\_\_\_  
Date Signed

\_\_\_\_\_  
Agency Name

## Appendix B

### Reporting Template



*Governor's Community Outreach - Federal Programs Office*

### Personally Identifiable Information

### Actual or Imminent Breach Reporting Form

1. Breach Reported by:			
Agency:			
Name:		Supervisor:	
Email:		Email:	
Phone:		Phone:	

2. Breach Response Team:			
Name:		Name:	
Email:		Email:	
Phone:		Phone:	
Name:		Name:	
Email:		Email:	
Phone:		Phone:	
Name:		Name:	
Email:		Email:	
Phone:		Phone:	

3. Breach Summary:	
Date and Time of Breach:	
Location Breach:	
Do not include PII or classified information. Summarize the facts of circumstances of the theft, loss, or compromise of PII as currently known, including:	
a. A description of the parties involved in the breach;	
b. The physical or electronic storage location of the information at risk;	

c. If steps were immediately taken to contain the breach;

d. Whether the breach is an isolated occurrence or a systematic problem;

e. Who conducted the investigations of the breach, if applicable; and

f. Any other pertinent information.

4. Type of Breach:			
Lost Information or Equipment	<input type="checkbox"/>	Unauthorized Disclosure	<input type="checkbox"/>
Stolen Information or Equipment	<input type="checkbox"/>	Unauthorized Access	<input type="checkbox"/>
Unauthorized Equipment  (e.g., using an unauthorized personal device, server, or email account to store PII)	<input type="checkbox"/>	Unauthorized Use  (e.g., employee with agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)	<input type="checkbox"/>

5. Storage Medium:			
Laptop or Tablet	<input type="checkbox"/>	Smartphone	<input type="checkbox"/>
Desktop	<input type="checkbox"/>	Paper files	<input type="checkbox"/>
External Storage Device	<input type="checkbox"/>	External Storage Device (e.g., CD, DVD, USB Drive, etc.)	<input type="checkbox"/>
IT System (Intranet/Shared Drive)	<input type="checkbox"/>	Oral Disclosure	<input type="checkbox"/>
Email:			
Type of Breached Personal Information:			
Other:			

6. Reported to	
<b>1. Agency Name:</b>	
Name:	
Title:	
Email:	
Phone:	
Date and time of the report:	
<b>2. Agency Name:</b>	
Name:	
Title:	
Email:	
Phone:	
Date and time of the report:	
<b>3. Agency Name:</b>	
Name:	
Title:	
Email:	
Phone:	
Date and time of the report:	

7. Data Elements and Information Types (select all that apply)		
<b>Stand Alone Identifying Numbers</b>		
<b>A</b>		
Social Security number <input type="checkbox"/>	Driver's license, state ID numbers <input type="checkbox"/>	
Passport numbers <input type="checkbox"/>	Alien Registration numbers <input type="checkbox"/>	
Financial account numbers <input type="checkbox"/>	Biometric identifiers <input type="checkbox"/>	
<i>When Stand Alone information is used in combination with any of the following:</i>		
<b>Biographical Information</b>		
<b>B</b>		
Name (including nicknames) <input type="checkbox"/>	Gender <input type="checkbox"/>	Race <input type="checkbox"/>
Date of Birth (Day, Month, Year) <input type="checkbox"/>	Ethnicity <input type="checkbox"/>	Nationality <input type="checkbox"/>
Country of Birth <input type="checkbox"/>	City or County of Birth <input type="checkbox"/>	Marital Status <input type="checkbox"/>
Citizenship <input type="checkbox"/>	Immigration Status <input type="checkbox"/>	Religion/Religious Preference <input type="checkbox"/>
Home Address <input type="checkbox"/>	Zip Code <input type="checkbox"/>	Home Phone or Fax Number <input type="checkbox"/>
Spouse Information <input type="checkbox"/>	Sexual Orientation <input type="checkbox"/>	Children Information <input type="checkbox"/>
Group/Organization Membership <input type="checkbox"/>	Military Service Information <input type="checkbox"/>	Mother's Maiden Name. <input type="checkbox"/>
Business Mailing Address (sole proprietor) <input type="checkbox"/>	Business Phone or Fax Number (sole proprietor) <input type="checkbox"/>	Global Positioning System (GPS)/Location Data <input type="checkbox"/>
Personal e-mail address. <input type="checkbox"/>	Business e-mail address <input type="checkbox"/>	Employment Information. <input type="checkbox"/>
Education Information. <input type="checkbox"/>	Resume or curriculum vitae <input type="checkbox"/>	Professional/personal references <input type="checkbox"/>
<b>Biometrics/Distinguishing Features/Characteristics</b>		
<b>C</b>		
Fingerprints <input type="checkbox"/>	Palm prints <input type="checkbox"/>	Vascular scans <input type="checkbox"/>
Retina/Iris Scans <input type="checkbox"/>	Dental Profile <input type="checkbox"/>	Scars, marks, tattoos <input type="checkbox"/>
Hair Color <input type="checkbox"/>	Eye Color <input type="checkbox"/>	Height <input type="checkbox"/>
Video Recording <input type="checkbox"/>	Photos <input type="checkbox"/>	Voice/Audio Recording <input type="checkbox"/>
DNA Sample or Profile <input type="checkbox"/>	Signatures <input type="checkbox"/>	Weight <input type="checkbox"/>
<b>Medical/Emergency Information</b>		
<b>D</b>		
Medical/Health Information <input type="checkbox"/>	Mental Health Information <input type="checkbox"/>	Disability Information <input type="checkbox"/>
Workers' Compensation Information <input type="checkbox"/>	Patient ID Number <input type="checkbox"/>	Emergency Contact Information <input type="checkbox"/>
<b>Device Information</b>		
<b>E</b>		
Device settings or preferences (e.g., security level, sharing options, ringtones) <input type="checkbox"/>	Cell tower records (e.g., logs, user location, time, etc.) <input type="checkbox"/>	Network communications data <input type="checkbox"/>
<b>Specific Information / File Types</b>		
<b>F</b>		
Taxpayer Information/Tax Return Information <input type="checkbox"/>	Law Enforcement Information <input type="checkbox"/>	Security Clearance/Background Check Information <input type="checkbox"/>
Civil/Criminal History Information/Police Record <input type="checkbox"/>	Academic and Professional Background Information. <input type="checkbox"/>	Health Information <input type="checkbox"/>
Case Files <input type="checkbox"/>	Personnel Files <input type="checkbox"/>	Credit History Information. <input type="checkbox"/>

8. FOR GCO-FPO USE ONLY		
Staff Receiving this Report:		
Name:		
Email:		
Phone:		
Date and time report received:		
Reporting to Grantor:		
Reported to Grantor Agency and Agency Name:		
Name:		
Method:	Email	Phone
Date and time:		
Information reported:		

Action to be taken:					
Notes for subgrantee & follow-up:					
<b>9. Grantor Approved Status Closure:</b>					
Approved by:				Date and time:	
Documentation on hand:			Cross filed: (e.g., project and mother folder)		
<b>10. GCO-FPO Certification</b> <small>(Certify when matters have been fully closed and/or resolved)</small>					
Administrator Signature:					
Date:					